UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-00101	6007

28875 7590 01/07/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,231	MATT, BRIAN J.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: The specification appears to contain minor errors. For example, in paragraph 0057 (page 14, lines 4 and 5), it appears that references to "node 120" are intended to refer to "node 110". Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

2. Claims 2, 19, and 21 are objected to because of the following informalities:

Claim 2 recites the limitation "verifying the hash value at the second node" in both lines 14 and 23. In light of the specification and claim 11, it appears that one of these recitations, most likely the second, is intended to read "verifying the hash value at the first node". Similarly, Claim 19 recites the limitation "verifying the hash value at the second node" in both lines 15 and 23, and Claim 21 recites the limitation of a "verifying mechanism that is configured to verify the hash value at the second node" in lines 16-17 and 24-25. It appears that the second recitation of each of these limitations is intended to read "first node" in place of "second node".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al, *Handbook of Applied Cryptography*.

In reference to Claim 1, Menezes discloses the Needham-Schroeder key distribution protocol, a method that includes requesting establishing a cryptographic key between a first node and a second node, sending a message from the second node to a key distribution center that includes identifiers for the nodes (page 503, protocol 12.26, message 1), generating a cryptographic key at the key distribution center, and communicating the cryptographic key to the first and second nodes (page 503, protocol 12.26, message 2). Although the protocol does not explicitly disclose the use of message authentication codes, or recreating a second node key previously created using the second node identifier and a secret key of the key distribution center, Menezes discloses both MACs (see page 361, below definition 9.77) and identity-based keying (page 561, section 13.4.3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the key distribution protocol by including the use of a MAC, in order to provide data origin authentication and data integrity (see Menezes, page 361, definition 9.77) and by including identity-

based keying, in order to prevent forgery and impersonation (see Menezes, page 561, section 13.4.3).

In reference to Claim 2, Menezes further discloses communicating the cryptographic key to the nodes by encrypting the cryptographic key using the second node key to form a first encrypted key, encrypting the cryptographic key using the first node key to form a second encrypted key, sending a message from the key distribution center to the second node that includes the first and second encrypted keys (page 503. protocol 12.26, message 2), decrypting the first encrypted key at the second node to recover the cryptographic key, sending the second encrypted key and a key confirmation value to the first node (page 503, protocol 12.26, messages 3 and 5), decrypting the second encrypted key at the first node to recover the cryptographic key, establishing at the first node that the second node has the cryptographic key using the key confirmation value, and sending a message to the second node from the first node so the second node can establish that the first node has the cryptographic key (page 503, protocol 12.26, message 4). Although the protocol does not explicitly disclose recreating a first node key previously created using the first node identifier and the secret key, Menezes discloses identity-based keying (page 561, section 13.4.3). Further, although the protocol does not explicitly disclose the use of a hash value in the messages for verification, Menezes discloses that hash values can be used for verification of data (see, for example, page 322, first full paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made

to further modify the key distribution protocol by including the use of a hash, in order to provide data integrity (see Menezes, pages 321-322, section 9.1).

In reference to Claims 3 and 4, Menezes further discloses that the messages include the node identifiers and a nonce (page 503, protocol 12.26, message 1).

In reference to Claim 5, Menezes further discloses verifying the message authentication code by creating a test MAC to compare with the original MAC (pages 321-322, section 9.1).

In reference to Claim 6, 8, and 11, Menezes further discloses verifying the hash value by creating a hash value and creating test hash values to compare with the original hash value (page 322, first full paragraph).

In reference to Claim 7, Menezes further discloses that a message includes the node identifiers and the encrypted keys (page 503, protocol 12.26, message 2).

In reference to Claims 9 and 10, Menezes further discloses that a message includes identifiers, a nonce, and a confirmation value that includes an encrypted nonce (page 503, protocol 12.26, message 5).

In reference to Claims 12 and 15, Menezes discloses that each node confirms that the other has the cryptographic key by verifying nonces (page 503, protocol 12.26, messages 4 and 5).

In reference to Claims 13 and 14, Menezes further discloses that a message includes identifiers and an encrypted confirmation value (page 503, protocol 12.26, message 4).

In reference to Claims 16 and 17, Menezes discloses identity-based keying (page 561, section 13.4.3) and that the node keys are installed in the node prior to deployment (page 503, protocol 12.26, "One-time setup").

Claims 18 and 19 are directed to software implementations of the methods of Claims 1 and 2, and are rejected by a similar rationale.

Similarly, Claims 20 and 21 are directed to an apparatus corresponding substantially to the methods of Claims 1 and 2, and are rejected by a similar rationale.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Schneier, *Applied Cryptography*, also discloses many key distribution schemes, message authentication codes, hashes, and identity-based keying.

b. Bellare et al, US Patent 5491750, discloses a method for authentication and key distribution including message authentication codes.

c. Shamir, "Identity-Based Cryptosystems and Signature Schemes", discloses the use of identification information as part of keying and signature material.

d. Gunther, "An Identity-Based Key-Exchange Protocol", discloses an identity-based system for establishing keys through a key authentication center.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER